Engineering and Technology Journal
Journal homepage: https://etj.uotechnology.edu.iq

The Evaluation of Time-Dependent Initialization Vector Advanced Encryption Standard Algorithm for Image Encryption

Hayder T. Assafli[a] *, Ivan A. Hashim[a], Ahmed A. Naser[b]

[a] Electrical Engineering Dept, University of Technology-Iraq, Alsina'a street, 10066 Baghdad, Iraq.
[b] Directorate of Space and Communication, Ministry of Science and Technology, Baghdad, Iraq
*Corresponding author Email: hayder.t.assafli@uotechnology.edu.iq

HIGHLIGHTS

- Sensitive data has to be protected from the public.
- A strong encryption algorithm is required for protecting images.
- Computing speed is growing, making algorithms vulnerable to attacks.
- An enhanced AES-CBC algorithm is evaluated for the encryption proposed.
- The algorithm satisfied the required standards and passed all tests.

ARTICLE INFO

Handling editor: Jawad K. Ali

Keywords:
Advanced Encryption Standard; Cipher Block Chaining; Epoch time; Image encryption; Time-dependent.

ABSTRACT

The Advanced Encryption Standard (AES) has become an attractive encryption method for high security and fast implementation. The encryption algorithm is approved as a standard for widely-used communication and data processing units. However, the advance in technology and the introduction of quantum computers made the encryption scheme vulnerable to attack. Different attack procedures are continuously developed to attack end decrypted important and sensitive data. This paper evaluated an enhanced Advanced Encryption System operating in Cipher Block Chaining mode, suggesting a promising solution for resisting future attacks. The approach depends on a time-dependent initialization vector that produces the initialization vector block depending on the epoch time without sharing any encryption key. The evaluation process includes correlation analysis, global and local Shannon entropy analysis, chi-square analysis, histogram analysis, and differential analysis. The results showed that the enhanced encryption scheme is reliable and can resist most cyber-attacks without exposing any encrypted data to the public. The results were compared with previously published and tested algorithms and found to satisfy and exceed the minimum requirement. So, the encryption method can be implemented safely in future communication channels or used in the file encryption process.

1. Introduction

The privacy of private information has become a major concern recently. Multimedia content such as videos, audio, and images is some of the major content in social media and contains personal information that must be protected from blackmailing or unauthorized use. Moreover, the growing technology made images one of the most important contests that carry valuable information in several majors such as commercial, political, military, and medicine. These contents usually are transferred through encrypted channels, or the media itself is encrypted before sending. However, advances in technology and computing speed exposed these contents to hacking by finding the encryption key using different techniques. This paper addresses a major problem and suggests an encryption scheme that does not require sharing any encryption key.

Moreover, the suggested technique can be used in addressing or limiting the time for decrypting certain information. The rest of this paper is organized as follows: Section 2 cites previous work related to this subject. In Section 3, the AES encryption with the proposed enhancement is explained. Section 4 represents the simulation results and the techniques used to analyze the encryption algorithm. Finally, section 5 gives a comprehensive summary of this paper.

Several encryption algorithms have been developed during the last century, such as DES, Triple DES, AES, IDEA, etc. However, some of these algorithms are not secure for image encryption [1-3]. Recently, various enhancements have been proposed for image encryption algorithms. For example, the Advanced Encryption Algorithm depends on a static substitution box for introducing nonlinearity into the encryption process. This static substitution box can be replaced by a dynamic box that changes its contents according to certain parameters such as RC4 [4]. An S-box is generated depending on the RC4 stream cipher.

http://doi.org/10.30684/etj.2021.131397.1032
Received 6 September 2021; Accepted 12 December 2021; Available online 3 June 2022
2412-0758/University of Technology-Iraq, Baghdad, Iraq

.

The resulting S-box is dynamic and depends on the encryption key, increasing the linear and differential cryptanalysis by adding more complexity to the encryption process. This enhancement helps to protect encrypted images from decryption by constantly changing the s-box. On the other hand, the image itself may contain information that helps protect it from decryption, such as chaotic encryption for RGB-colored images [5]. This method encrypts each color depending on the other colors' horizontal, vertical, and diagonal correlation. The algorithm decreases the correlation between the three color components and makes the encrypted image more immune to attacks. Another research suggests that the safety and security of the AES algorithm are increased by generating a random key and permutation keys in the AES rounds [6]. This process replaces the regular key expansion process of the AES encryption. The randomness of the key generation process is preserved by the round permutation. Also, high confusion and diffusion are introduced into the AES algorithm by implementing a key-dependent S-box without altering the block size keys [7]. The drawback of this type is that it consumes more logic elements and costs more time during execution.

In another work, the implementation of a dynamic S-box is inspired by the bee colony algorithm for increasing the resistance against attacks [8]. The bee colony algorithm is an artificially intelligent algorithm containing a random variable passed to the permutation box during each run resulting in a different S-box. The cipher feedback mode can also be modified to improve the efficiency, speed, and performance of the encryption [9]. In this enhancement, the cipher feedback mode is modified to produce a different key block after each key generating step during the substitute byte and shift rows process. Modifying the substitution box has an important influence on the encryption process because of the nonlinearity effect. Dynamic irreducible polynomial and affine constants also implement dynamic key-dependent substitution boxes [10]. The applied methodology produces 256 different s-boxes by changing only one bit in the encryption key. The resulted algorithm was analyzed and produced desired encryption strength results. On the other hand, other suggested enhanced s-box algorithms do not depend on a key or external parameter [11]. The initial s-box can be considered a starting point, and the succeeding s-boxes all depend on the initial s-box, such as the APA s-box, S8 AES s-box[12], and Gray s-box[13].

Other enhancements can be made to increase the efficiency of the encryption process, such as increasing the processing speed by reducing the encryption. Furthermore, different hardware platforms can accelerate the encryption process by using GPUs as an alternative to CPUs, such as in [14]. Furthermore, the programming language also influences the speed of the encryption process, such as using OpenCL [15] or CUDA [16]. Finally, time-dependent modifications are used to introduce a new changing parameter to the encryption process, which will be analyzed in this paper [17]. The main contribution of this work is to evaluate the encryption algorithm that depends on the time-dependent Initialization Vector by calculating image encryption parameters. Moreover, the algorithm is tested for passing the National Institute of Standard and Technology (NIST) statistical randomness test [18–20].

2. Advanced Encryption Standard

Advanced Encryption Standard encryption algorithm was created in 1997 by V. Rijman and J. Daemen. It is a 128-bit length block cipher algorithm. The encryption process consists of four basic processes that are repeated through several rounds depending on the length of the encryption key: 10 rounds for 128 bit, 12 rounds for 192 bit, and 14 rounds for 256-bit keys. First, the number of rounds is derived from the cipher key length. Then, the state arrays are initialized from the plaintext data to start the rounds operation process. In the beginning, the AddRoundKey step is applied. Next, a simple XOR operation is performed between the encryption key and the data block in this process. Then, four operations are executed repeatedly between the initial and final rounds. These operations are applied to the data block or state to add confusion and introduce nonlinearity to the encryption process. The first process starts with a subByte. In this step, each byte is replaced with another byte depending on a substitution box that introduces the highest nonlinearity among all other steps. Then, the ShiftRows operation is applied, which performs circular shifting across each row in the state matrix. After that, the MixColumns process performs mixing between the columns to add more confusion to the state block. Finally, the AddRound key is applied between the encryption key and the state block. The final round is completed with only three processes instead of four by excluding the MixColumns process. The output of the rounds is an encrypted state array called ciphertext that can be transmitted safely. Figure 1 shows the complete 128-bit AES encryption process [21].

3. Methodology

An enhanced encryption algorithm is used to encrypt images and evaluate the results. The encryption algorithm depends on epoch time as a nonce number for the initialization vector [22]. The enhanced encryption algorithm is never tested for image encryption purposes. The time-dependent algorithm depends on the epoch time transmitted globally by GPS satellite systems [23]. The epoch or Unix time is a non-repetitive 32-bit number transmitted and synchronized across the globe and reflects the elapsed time in seconds since the Unix epoch, which is January 1st, 1970. These bits are used as a source for the Initialization Vector. The selection of the bits results in different encryption combinations resulting in a completely different ciphertext. The selected bits and the change of each bit is only known to the sender and receiver. The update of the bit combination can be done on hourly, daily, weekly, or yearly bases. This property can also be sued as a time limit. In other words, the encrypted information cannot be decrypted after a certain time. This work investigates and evaluates the strength of the encryption algorithm for image encryption purposes. Various images are used as data sources such as Lena, Cameraman, Mandrill, Truck, Living-room, Pirate, Barbara, Woman, and Peppers. The results of each encryption process are evaluated using numerous evaluation techniques such as histogram analysis, correlation analysis between two adjacent pixels, chi-square analysis, global entropy analysis, local entropy analysis, key sensitivity analysis, and differential attack analysis. As shown in Figure 2, a time-dependent initialization vector is used for initiating the Advanced Encryption Standard - Cipher Block Chaining mode (AES-CBC). This process ensures different results after each encryption operation without changing the encryption key.

4. Encryption Results and Analysis

4.1 Histogram analysis

An image's histogram represents the distribution of color or grayscale tone among digital pixels. In any image, the histogram shows that some pixels have a higher number of tones than others, reflecting digital information about the image. However, the encryption process distributes the tones evenly between the pixels as possible. So, the original image is completely replaced by an encrypted image with evenly distributed tones among pixels [24]. The histogram test results are illustrated in Figure 3. The next column shows the original image histogram, and the fourth column of the same figure shows the histogram of each encrypted image. It can be seen that all encrypted images have well-distributed tones indicating their resistance to statistical attacks.

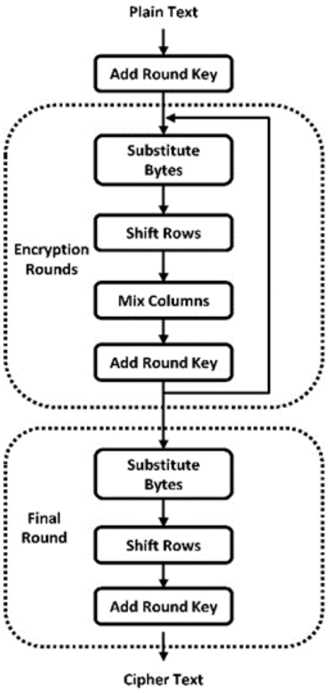

Figure 1: The AES encryption process

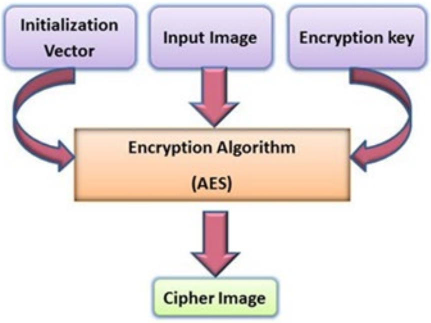

Figure 2: The Initialization Vector for AES-CBC

4.2 Chi-square analysis

The Chi-square analysis estimates the distribution of the encrypted pixel values using Eq. (1):

$$\chi^2_{test} = \sum_{i=1}^{k} \frac{(o_i - e_i)^2}{e_i} \tag{1}$$

Where k is the maximum intensity (256 for gray pixels), o_i is the repetition occurrence of each gray value taken from the image, and e_i is the estimated repetition occurrence of each pixel value [25]. The results of the encryption test are shown in Table

1. These results illustrate that the encrypted images have uniform distribution because the calculated chi-square values are less than the theoretical value of 293.24783 [26].

4.3 Correlation analysis of two adjacent pixels

This analysis calculates the correlation between adjacent pixels by selecting random pairs from the original and encrypted images in vertical, horizontal, and diagonal directions. Then, the correlation factor is calculated by Eq. (2) - Eq. (5) [27]:

$$r_{xy} = \frac{cov\ (x,y)}{s_x s_y} \tag{2}$$

Where:

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x)(y_i - E(y)) \tag{3}$$

$$s_x = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2} \tag{4}$$

And

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{5}$$

The correlation distribution for adjacent pixels from the Lena color image and the encrypted image is shown in Figure 4.

There is no correlation among adjacent pixels for each color in the encrypted image, as shown in Figure 4. Moreover, the correlation coefficients for the rest of the images show that the encryption approach is resistive to statistical attack, as listed in Table 2.

4.4 Information entropy analysis

Information entropy is one of the important encryption evaluation parameters. It evaluates the encrypted image by estimating the randomness between the image pixels according to Eq. (6) [31]:

$$W(s) = \sum_{i=0}^{2^k-1} f(s_i) log_2 \frac{1}{f(s_i)} \tag{6}$$

Where k is the depth of the bit of the image and f(si) is the probability of distribution of the bit depths across the image pixels. According to the results obtained from the encrypted images, the information entropy is high and near the ideal theoretical value of 8. So, the encryption method satisfies the entropy requirement, as shown in Table 3.

The local information Shannon entropy is also calculated using Eq. (7) [33]:

$$\overline{W_{k,Tb}}(C) = \sum_{i=1}^{k} \frac{W(C_i)}{k} \tag{7}$$

This evaluation method takes a number (k) of non-overlapping blocks with the number of pixels Tb from the ciphered image. Then, the mean Shannon entropy is evaluated before summing them up together. This method has several advantages in overcoming the weakness of global Shannon entropy calculations. For example, table 4 shows that all the images passed the local Shannon entropy test for local information significance level α = 0.05 [28]. The test parameters taken from [34] were 30 and 1936 fork and Tb, respectively.

Table 1: Chi-square test results

Image	Plain image	Proposed	Result
Lena	293.24783	260.36719	Passed
Mandril	293.24783	288.96680	Passed
Cameraman	293.24783	202.28711	Passed
Living-room	293.24783	258.75195	Passed
Pirate	293.24783	251.61914	Passed
Woman	293.24783	240.07617	Passed
Truck	293.24783	262.22266	Passed
Peppers	293.24783	234.23242	Passed
Barbara	293.24783	268.04102	Passed

Table 2: Correlation between adjacent pixels

Image	Direction	Original Image	Encrypted Image				
			Proposed	Ref. [26]	Ref. [28]	Ref. [29]	Ref. [30]
Lena	H	0.9688	-0.0010	0.0106	0.0210	-0.0070	-0.0070
	V	0.9832	-0.0030	-0.0012	0.0038	-0.0054	0.0151
	D	0.9721	0.0025	0.0009	-0.0042	0.0055	0.0003
Mandril	H	0.8665	-0.0016	0.0230	0.0042	0.0112	0.0064
	V	0.7587	0.0010	0.0054	-0.0152	0.0006	-0.0138
	D	0.7262	-0.0015	-0.0168	-0.0051	-0.0019	0.0087
Cameraman	H	0.9771	0.0143	0.0113	0.0157	-0.0003	0.0033
	V	0.9901	0.0008	0.0169	-0.0139	0.0037	0.0027
	D	0.9815	-0.0030	0.0034	0.0064	-0.0048	0.0122
Living room	H	0.9606	0.0009	0.0100	-0.0043	0.0007	0.0350
	V	0.8926	-0.0007	0.0114	0.0157	-0.0079	0.0359
	D	0.9586	0.0010	-0.0025	-0.0038	0.0003	0.0047
Pirate	H	0.9591	0.0049	-0.0251	0.0144	0.0048	0.0315
	V	0.9727	-0.0321	-0.0108	0.0157	0.0033	0.0114
	D	0.9630	0.0141	-0.0326	0.0054	0.0156	0.0174
Woman	H	0.9487	0.0236	0.0172	0.0056	-0.0085	0.0245
	V	0.9662	-0.0120	0.0017	0.0080	0.0087	0.0070
	D	0.9402	-0.0173	0.0013	0.0036	0.0106	0.0118
Truck	H	0.9619	-0.0018	-0.0060	0.0083	-0.0046	0.1004
	V	0.9311	0.0235	-0.0089	0.0043	-0.0088	0.0651
	D	0.9607	-0.0098	-0.0146	0.0049	0.0030	0.0452
Peppers	H	0.9831	-0.0354	-0.0024	0.0070	-0.0006	-0.0070
	V	0.9850	0.0109	0.0142	0.0137	0.0114	0.0151
	D	0.9774	-0.0080	-0.0050	0.0039	0.0179	0.0003
Barbara	H	0.8743	0.0186	0.0040	0.0058	0.0076	0.0033
	V	0.9548	-0.0531	0.0024	0.0004	0.0105	0.0027
	D	0.8429	-0.0140	0.0006	0.0027	0.0050	0.0122

4.5 Differential attack

To calculate the ability of the algorithm to resist differential attack, the NPCR and UACI are estimated from Eq. (8) - Eq. (10) [34]:

$$NPCR = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} D(i,j)}{m \times n} \times 100\% \tag{8}$$

$$(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j) \\ 1, & C_1(i,j) \neq C_2(i,j) \end{cases} \tag{9}$$

$$UACI = \frac{1}{m \times n}\left(\sum_{i=1}^{m}\sum_{j=1}^{n} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right) \times 100\% \tag{10}$$

Where P1 is the original image and C1 is the encrypted image. P2 is the original image with the one-bit difference from P1, and C2 is the one-bit different encrypted image. By examining Table 5, the NPCR for a 512 x 512 grayscale image is nearly the ideal value of 99.6094%. Additionally, the UACI is also very close to the theoretical value of 33.4635% [35]. This shows that the scheme is resistive to differential attacks.

4.6 The nist statistical test

The NIST Statistical Test Suit is a standard evaluation tool developed for estimating the randomness of the generated sequence [18,19]. The tool consists of 15 tests that check the p-value significance at each run. If the result of the p-value passes the 0.01 level, the sequence passes the randomness test. The test suit is used to test the randomness of different algorithms [36-37]. Several NIST test runs have been applied for different images at different times. All results showed that the change in time does not affect the randomness of the generated sequence. Table 6 shows the results of the first 1000000 bits stream of the encrypted Lena image.

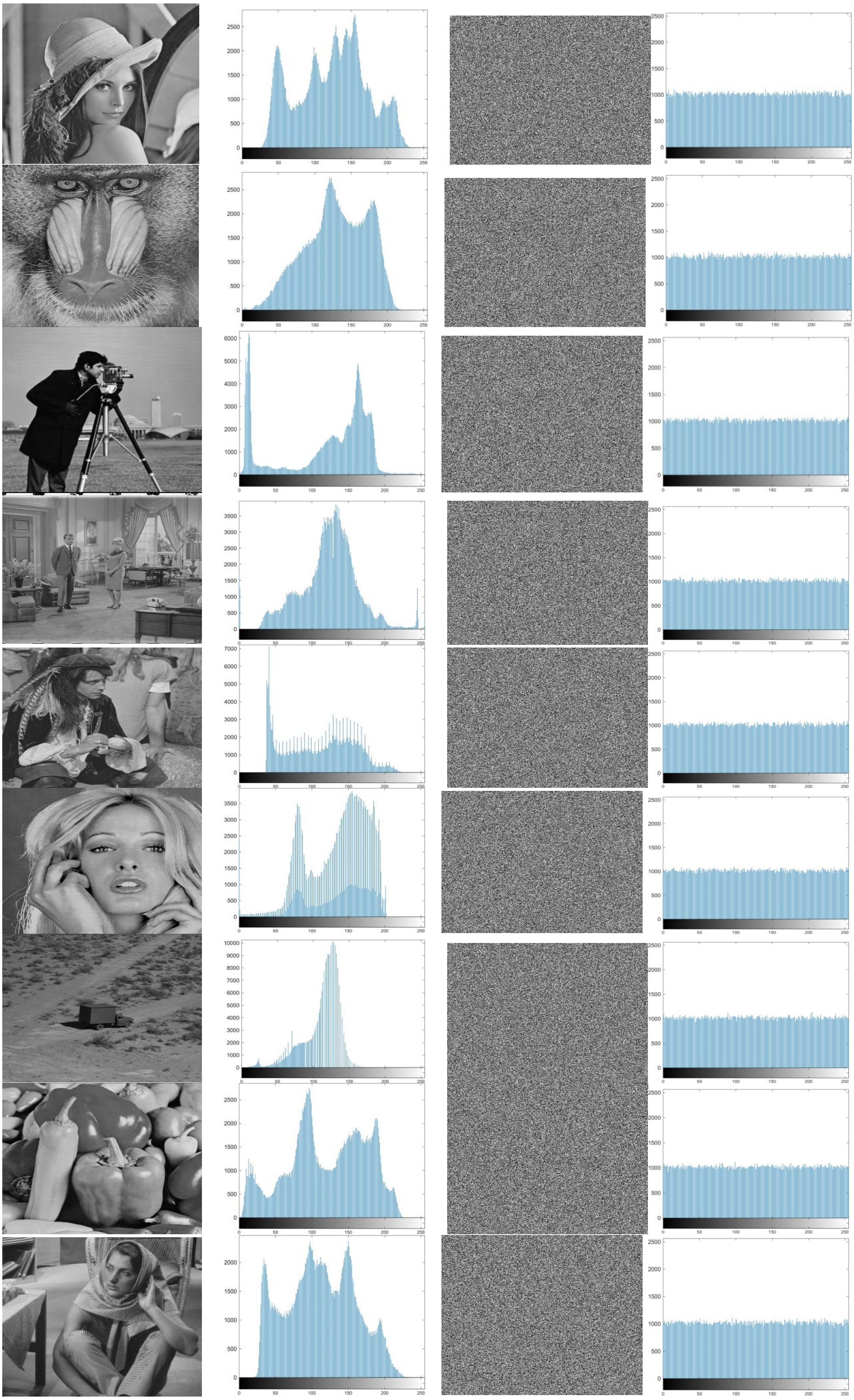

Figure 3: The histogram of original and encrypted images

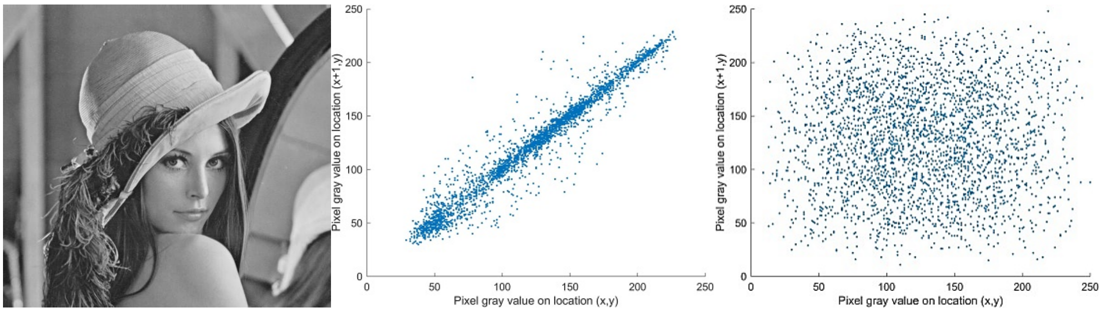

Figure 4: The correlation between adjacent pixels for original and encrypted Lena image

Table 3: Global entropy test results

Image	Original Image	Proposed	Ref. [26]	Ref. [32]	Ref. [28]	Ref. [29]	Ref. [30]
Lena	7.4451	7.9993	7.9972	7.9969	7.9973	7.9967	7.8963
Mandril	7.3583	7.9992	7.9967	7.9966	7.9975	7.9972	7.9007
Cameraman	7.0480	7.9994	7.9972	7.9970	7.9972	7.9973	7.8979
Living-room	7.2010	7.9993	7.9971	7.9973	7.9975	7.9975	7.8973
Pirate	7.2367	7.9993	7.9974	7.9974	7.9970	7.9973	7.8973
Woman	6.9542	7.9993	7.9976	7.9973	7.9968	7.9968	7.8977
Truck	6.0274	7.9993	7.9975	7.9969	7.9970	7.9969	7.8944
Peppers	7.5937	7.9994	7.9971	7.9972	7.9972	7.9976	7.8992
Barbara	7.4664	7.9993	7.9969	7.9970	7.9973	7.9973	7.9003

Table 4: Local Shannon entropy test results

7	Local Shannon Entropy of the encrypted image	Test results
Lena	7.9032	Pass
Mandril	7.9005	Pass
Cameraman	7.9022	Pass
Living-room	7.9031	Pass
Pirate	7.9022	Pass
Woman	7.9028	Pass
Truck	7.9026	Pass
Peppers	7.9021	Pass
Barbara	7.9027	Pass

Table 5: The NPCR and UACI results

Image	NPCR				UACI			
	Proposed	Ref. [26]	Ref. [28]	Ref. [29]	Ref. [22]	Ref. [26]	Ref. [28]	Ref. [29]
Lena	99.6258	99.6216	99.6246	99.6262	33.4440	33.4994	33.4877	33.4010
Mandril	99.6048	99.6368	99.6246	99.6094	33.3768	33.4702	33.5104	33.4461
Cameraman	99.6311	99.6353	99.5926	99.6185	33.4139	33.4810	33.4269	33.4231
Living-room	99.5888	99.6414	99.6063	99.6475	33.3672	33.4871	33.5146	33.4581
Pirate	99.6349	99.5773	99.6643	99.6170	33.4246	33.5008	33.4994	33.4387
Woman	99.6006	99.6246	99.6155	99.6140	33.3128	33.5307	33.4664	33.4808
Truck	99.6281	99.6246	99.5926	99.6246	33.4383	33.4672	33.4964	33.5324
Peppers	99.5983	99.5865	99.6307	99.5834	33.4211	33.4815	33.5047	33.4827
Barbara	99.6048	99.6078	99.6170	99.6231	33.3386	33.4894	33.4771	33.4643

Table 6: NIST Randomness Tests of the proposed algorithm

Test	P-value	Results
Frequency	0.891821	Pass
Block frequency	0.549445	Pass
Cumulative sums	0.787595	Pass
Runs	0.562022	Pass
Long runs of ones	0.281720	Pass
Rank	0.972436	Pass
Discrete Fourier transform	0.963403	Pass
Non-overlapping template matching	0.774769	Pass
Overlapping template matching	0.240871	Pass
Maurer’s universal statistical	0.846932	Pass
Approximate entropy	0.823434	Pass
Random excursions	0.645428	Pass
Random excursions variant	0.581289	Pass
Linear complexity	0.841542	Pass
Serial	0.313112	Pass

4.7 Speed Performance Test

Since the modification has been done before executing the AES-CBC algorithm, the speed performance and analysis stay constant depending on the hardware platform. A complete speed evaluation has been done with throughput calculation [36–38].

5. Conclusion

This paper explains and evaluates a time-dependent Advanced Encryption Standard in Cipher Block Chaining mode. The enhanced algorithm depends on the epoch time as an initialization vector. This initialization vector can be assigned bites from the time-dependent Unix time. Several standard images are used for the analysis processes, tested before and after encryption at different times. The ciphered images are analyzed using correlation analysis, global and local Shannon entropy analysis, chi-square analysis, differential analysis, and histogram analysis. The results showed that the encryption method satisfies the standard requirements and can stand against attacks.

Moreover, the NIST test results showed that the algorithm passes all randomness tests. Therefore, further investigations can be done to quantify the algorithm for the encryption of streaming data for future work. Additionally, the approach can be implemented on a hardware platform, such as FPGA and tested for real-time operation.

Author contribution

Conceptualization, I. Hashim, A. Naser, and H. Assafli; methodology, I. Hashim and H. Assafli.; software, H. Assafli.; validation, H. Assafli., H. Assafli.; formal analysis, H. Assafli.; investigation, H. Assafli.; resources, H. Assafli.; data curation, H. Assafli and I. Hashim.; writing—original draft preparation, H. Assafli.; writing—review and editing, I. Hashim, A. Naser and H. Assafli.; visualization, H. Assafli.; supervision, I. Hashim, A. Naser and A. Naser. All authors have read and agreed to the published version of the manuscript

Funding

This research received no external funding.

Conflicts of interest

The authors declare no conflict of interest.

References

[1] G. Alvarez , S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, Int. J. Bifurc. Chaos, 16 (2006) 2129–2151. https://doi.org/10.1142/S0218127406015970

[2] R. Enayatifar, A. H. Abdullah, I. F. Isnin, Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence, Opt. Lasers. Eng., 56 (2014) 83–93. https://doi.org/10.1016/j.optlaseng.2013.12.003

[3] X. Wu, H. Kan, J. Kurths, A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps, Appl. Soft. Comput. J., 37 (2015) 24–39. https://doi.org/10.1016/j.asoc.2015.08.008

[4] S. Shivkumar , G. Umamaheswari, Performance Comparison of Advanced Encryption Standard (AES) and AES Key Dependent S-Box - Simulation Using MATLAB, Int. Conf. Process. Auto.. Cont. Comput., (2011) 1- 6 . https://doi.org/10.1109/PACC.2011.5979007

[5] X. Wang, L. Teng, X. Qin, A novel colour image encryption algorithm based on chaos, Signal Processing, 92 (2012) 1101–1108. https://doi.org/10.1016/j.sigpro.2011.10.023

[6] S. Habeeb, Proposal for Complex AES Security using key Generator and Text Permutation, Eng. Technol. J., 30 (2012) 2067–2075.

[7] S. Arrag, A. Hamdoun, A. Tragha, E. K. Salah, Implementation of stronger AES by using dynamic S-box dependent of master key, J. Theor. Appl. Inf. Technol., 53 (2013) 196–204.

[8] S. K. A. Kadhim, Proposal New S-box for AES Algorithm Depend on A.I Bee Colony, Eng. Technol. J., 33 (2015) 12–24.

[9] D. N. Hammod, M.A. Hamood Al-Rawi, H. S. Abdulah, An Enhancement Method Based on Modifying CFB Mode for Key Generation in AES Algorithm, Eng. Technol. J., 34 (2016) 759–768.

[10] P. Agarwal, A. Singh, A. Kilicman, Development of key-dependent dynamic S-Boxes with dynamic irreducible polynomial and affine constant, Adv. Mech. Eng., 10 (2018) 1–18. https://doi.org/10.1177/1687814018781638

[11] A. Y. Al-Dweik, I. Hussain, M. S. Saleh, M. T. Mustafa, A Novel Method to Generate Key-Dependent S-Boxes with Identical Algebraic Properties. (2019) 1–20. https://doi.org/10.48550/arXiv.1908.09168

[12] T. Naqash, A. Ishfaq, M. N. Ul-Islam, M. A. Hassan, U. Mujhaid, H. Mehmood, A novel mutual authentication protocol for H(e)NB and mobile devices using S8 S-box, Int. Conf. Syst. Technol., (2012) 56–59. https://doi.org/10.1109/ICOSST.2012.6472829

[13] M. T. Tran, D. K. Bui, A. D. Duong, Gray S-box for Advanced Encryption Standard, Int. Conf. Comput. Intell. Secur., 1 (2008) 253–258. https://doi.org/10.1109/CIS.2008.205

[14] H. T. Assafli, I. A. Hashim, A. A. Naser, Advanced Encryption Standard (AES) acceleration and analysis using graphical processing unit (GPU), Appl. Nanosci., 13 (2021) 1245–1250. https://doi.org/10.1007/s13204-021-01985-3

[15] T. Sanida, A. Sideris, M. Dasygenis, Accelerating the AES Algorithm using OpenCL, Int. Conf. Mod. Circuits Syst. Technol., (2020). https://doi.org/10.1109/MOCAST49295.2020.9200240

[16] A. A. Abdelrahman, M. M. Fouad, H. Dahshan, A. M. Mousa, High performance CUDA AES implementation: A quantitative performance analysis approach, Proc. Comput. Conf. 2017 (2018) 1077–1085. https://doi.org/10.1109/SAI.2017.8252225

[17] H. T. Assafli, I. A. Hashim, Generation and Evaluation of a New Time-Dependent Dynamic S-Box Algorithm for AES Block Cipher Cryptosystems, IOP Conf. Ser. Mater. Sci. Eng., 978 (2020) 012042. https://doi.org/10.1088/1757-899X/978/1/012042

[18] N. Sp , N. Sp, The NIST Statistical Test Suite, (2021) 1–6.

[19] M. Sýs , Z. Říha, Faster randomness testing with the NIST statistical test suite, Security, Privacy, Appl. Crypto. Eng. , 8804 (2014) 272–284. https://doi.org/10.1007/978-3-319-12060-7_18

[20] J. Zaman , R. Ghosh, Review on fifteen Statistical Tests proposed by NIST, Ijtpc, 1 (2012) 18–31.

[21] M. M. M.Nadzri, A. Ahmad A. Amira, Implementation of Advanced Encryption Standard (AES) for Wireless Image Transmission using LabVIEW, IEEE Student Conf. Res. Dev., (2018) 1–4. https://doi.org/10.1109/SCORED.2018.8710984

[22] H. T. Assafli , I. A. Hashim, Security Enhancement of AES-CBC and its Performance Evaluation Using the Avalanche Effect, Int. Conf. Eng. Technol. Appl., (2020) 7–11. https://doi.org/10.1109/IICETA50496.2020.9318803

[23] H. Y. Song , S. Hong, Investigating Cyclic Visit Pattern of Mobility Through Analysis of Geopositioning Data, 4 (2019) 589–602. Springer. Sci. Rev.,

[24] Z. Li, C. Peng, L. Li, X. Zhu, A novel plaintext-related image encryption scheme using hyper-chaotic system, Nonlinear Dyn., 94 (2018) 1319–1333. https://doi.org/10.1007/s11071-018-4426-4

[25] L. L. Huang, S. M. Wang, J. H. Xiang, A tweak-cube color image encryption scheme jointly manipulated by chaos and hyper-chaos, Appl. Sci., 9 (2019) 4854. https://doi.org/10.3390/app9224854

[26] L. Lidong, Y. Lei, D. Wang, A Fast Chaotic Image Encryption Scheme with Simultaneous Permutation-Diffusion Operation, IEEE Access., 8 (2020) 27361–27374. https://doi.org/10.1109/ACCESS.2020.2971759

[27] L. Liu, L. Zhang, D. Jiang, Y. Guan, Z. Zhang, A simultaneous scrambling and diffusion color image encryption algorithm based on hopfield chaotic neural network, IEEE Access, 7 (2019) 185796–185810. https://doi.org/10.1109/ACCESS.2019.2961164

[28] G. Ye, C. Pan, X. Huang, Q. Mei, An efficient pixel-level chaotic image encryption algorithm, Nonlinear Dyn., 94 (2018) 745–756. https://doi.org/10.1007/s11071-018-4391-y

[29] H. Diab, An Efficient Chaotic Image Cryptosystem Based on Simultaneous Permutation and Diffusion Operations, IEEE Access, 6 (2018) 42227–42244. https://doi.org/10.1109/ACCESS.2018.2858839

[30] R. I. Abdelfatah, Secure Image Transmission Using Chaotic-Enhanced Elliptic Curve Cryptography, IEEE Access, 8 (2020) 3875–3890. https://doi.org/10.1109/ACCESS.2019.2958336

[31] Y. Li, C. Wang, H. Chen, A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation, Opt. Lasers Eng., 90 (2017) 238–246. https://doi.org/10.1016/j.optlaseng.2016.10.020

[32] Y. Luo, R. Zhou, J. Liu, Y. Cao, X. Ding, A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map, Nonlinear Dyn., 93 (2018) 1165–1181. https://doi.org/10.1007/s11071-018-4251-9

[33] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, P. Natarajan, Local Shannon entropy measure with statistical tests for image randomness, Inf. Sci. ., 222 (2013) 323–342. htt ps://doi.org/10.1016/j.ins.2012.07.049

[34] J. Chen, Z. liang Zhu, L. bo Zhang, Y. Zhang, and B. qiang Yang, Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption, Signal. Process., 142 (2018) 340–353. https://doi.org/10.1016/j.sigpro.2017.07.034

[35] Y. Wu, J. P. Noonan, S. Agaian, NPCR and UACI Randomness Tests for Image Encryption, Cyberjournals.Com, 2011.

[36] E. Yavuz, R. Yazıcı, M. C. Kasapbaşı, E. Yamaç, A chaos-based image encryption algorithm with simple logical functions, Comput. Electr. Eng., 54 (2016) 471–483. https://doi.org/10.1016/j.compeleceng.2015.11.008

[37] Z. Hua, F. Jin, B. Xu, H. Huang, 2D Logistic-Sine-coupling map for image encryption, Signal. Process., 149 (2018) 148–161. https://doi.org/10.1016/j.sigpro.2018.03.010

[38] E. Yavuz, A novel chaotic image encryption algorithm based on content-sensitive dynamic function switching Optics .Laser Technol., 114 (2018) 224–239. https://doi.org/10.1016/j.optlastec.2019.01.043

[39] Y. Zhang, Test and Verification of AES Used for Image Encryption, 3D Res., 9 (2018). https://doi.org/10.1007/s13319-017-0154-7

[40] S. Amina and F. K. Mohamed, An efficient and secure chaotic cipher algorithm for image content preservation, Commun .Nonlinear. Sci. Numer. Simul., 60 (2018) 12–32. https://doi.org/10.1016/j.cnsns.2017.12.017